

BUMBLE BEE OPTIMIZATION ALGORITHM BASED OPTIMIZED DATA HIDING FOR IMAGE STEGANOGRAPHY

*Inderjeet Singh¹, Sarabjeet Kaur²

¹P.G. Student, Information Technology Department, Adesh Institute of Engineering & Technology, Faridkot, Punjab, India.

²Assistant Professor, Computer Science Engineering Department, Adesh Institute of Engineering & Technology, Faridkot, Punjab, India. (sarb7316@gmail.com)

*inder_handa007@yahoo.com

Abstract - The most important aspect of all forms of confidential communication is security. Although cryptography can be used to safeguard information, it also reveals the presence of covert communication. As a result, steganography, the art of secret communication, was devised. Steganography conceals the presence of covert communication by putting the secret information in a cover image. The inserting process generates the variability in the cover image that negatively impact the imperceptibility parameter. In order to enhance the imperceptibility parameter, bumble bee optimization algorithm based optimized data hiding method is proposed in this paper. The bumble bee optimization algorithm searches the optimal secret data order before data hiding. After determining the optimal secret data order, the data hiding is achieved using least significant bit (LSB) method. Besides that, in the proposed method, optimal cover image is also chosen by determining the 0's and 1's probability in the LSB of the cover image. The performance evaluation of the proposed method is done on five standard dataset images and various performance parameters are measured for it. The proposed method reduces the MSE and enhances the PSNR without impacting the embedding capacity.

Keywords - Bumble Bee Optimization Algorithm, Imperceptibility, Image Steganography, LSB, Security.

Manuscript Received: 25 Mar 2022, Accepted: 07 May 2022

DOI – 10.55083/irjeas.2022.v10i2005

© 2022 The authors. This is an open access article under the CC BY license. (<https://creativecommons.org/licenses/by/4.0/>)

1. INTRODUCTION

Since the previous several decades, the protection of confidential material has been a major focus of study, and this trend is expected to continue in the future. Information security has long relied on cryptography, the technique of scrambling data into a form that cannot be deciphered [1]. Cryptographic techniques, on the other hand, are hindered by the fact that encrypted communications are useless, trying to make them suspicious sufficiently draw the attention of adversaries, who may then decipher or modify the messages using strong cryptanalysis tools. Information masking technologies such as "steganography" may be used to secure confidential material throughout

transmission and minimize security problems. Originally from Greek, the term "steganography" refers to a method of concealing writing. In this particular area of information concealment, which is regarded as an art form, a hidden message is concealed behind a cover picture known only to the sender and the recipient. Carrier objects, embedding method, message and stego key are some of the core components of steganography, which may be used to encrypt and protect data. An image, audio, video, or text may be a carrier object [2-3]. In this paper, image is used as a cover image for data hiding. It is possible to employ steganography for a broad variety of purposes, such as the secure transmission of classified information among intelligence and military institutions and the



enhancement of mobile money services and polling security.

Least significant bit (LSB) is the most preferred algorithm in steganography [4]. In this method, the least significant bit of the cover media is replaced with secret data bit. This method is simpler, provides variability when cover media LSB bit is not matched with secret data bit. In order to reduce variability, various bio-inspired optimization algorithms are deployed for searching the optimal secret data order in the cover media for data hiding [5]. In the literature, the most preferred algorithms are deployed for steganography are genetic algorithm [6], particle swarm optimization [7], cuckoo search [8], cat swarm optimization [9], and Egyptian vulture optimization algorithm [10]. Out of these algorithms, genetic algorithm is maximum deployed for image steganography [11-13]. In the genetic algorithm, randomly populations are chosen for generate offspring's. Thus, if the selected population is not good then best offspring's can't generate from it. Further, some authors search the optimal cover image in place of secret data order for data hiding [14-15].

In this paper, we have searched the optimal cover image and determine the optimal secret data order to reduce the variability. To achieve this goal, we have deployed the bumble bee optimization algorithm for searching the optimal secret data order. The bumble bee optimization algorithm is superior over genetic algorithm because it performs the mating with best population to generate offspring's. The bumble bee optimization algorithm generates the different secret data order by flipping, circular shifting, reversing etc. After that, based on the objective function determined the optimal secret data order. In this work, we have taken PSNR as an objective function. Besides that, optimal cover image is also chosen from number of cover images by determining the 0's and 1's probability in the LSB of the cover image. After that, determining which cover image, 0's and 1's probability matched near about secret data order. After determining the optimal secret data order and cover image, the data hiding is done using LSB algorithm. The simulation evaluation is done using

MSE, PSNR, and embedding capacity. The results show that the proposed method provides lesser MSE, better PSNR and same embedding capacity as compared to Pratik D. Shah and Rajankumar S. Bichkar [15].

The rest of the paper is as follows. Section 2 explains the related work in which bumble bee optimization algorithm and least significant bit (LSB) algorithm. Section 3 illustrates the proposed method is designed to reduce variability in image steganography. Section 4 shows the simulation evaluation and comparative analysis with the existing methods. Conclusion and future scope are drawn in Section 5.

2. RELATED WORK

In the section, we have explained the bumble bee optimization (BBO) algorithm and least significant bit (LSB) algorithm in the proposed method. Out of these algorithms, BBO algorithm is deployed for determine the optimal secret data order whereas LSB algorithm is used to hide the optimal secret data order in the cover image. The detailed description of these algorithms is given below.

2.1 Bumble Bee Optimization Algorithm

This swarm intelligence algorithm is based on the behaviour of a swarm of bumble bees mating, and it mimics that behaviour. The BBMO algorithm is summarised as follows [16].

- **Initialization:** Using the initial random collection from bumble bees' population, the fitness of the population is calculated
- **Selection of Drones:** Queens choose the mating drones they like.
- **Origination of Offspring:** A new queen, a drone, and a worker are all subsets of the offspring that may be divided into three categories based on the manner of multiparent crossings used to create them.
- **Feeding the newly crowned queens:** Broods may be improved by using the "feeding technique," which can be used to identify areas for improvement.

The following equation illustrates how the new queen is fed by the old queen or the workers:

$$L_1 = (u_{bound} - l_{bound}) \times \left(w_1 - \frac{w_1}{iteration_{max}} \times t \right) + l_{bound} \quad (1)$$

$$L_2 = (u_{bound} - l_{bound}) \times \left(w_2 - \frac{w_2}{2 * iteration_{max}} \times t \right) + l_{bound} \quad (2)$$

"In this scenario, the term 'iteration' is used. The variables $L1$ and $L2$ have a range controlled by the parameters $w1$ and $w2$. There should be an increase in the value of $w2$ over $w1$ since value $L2$ should be greater than the value of $L1$ "
The formula for determining which feeding method to use is as follows:

$$tnq_i(t) = \begin{cases} q_i(t), & \text{if } rand_i(l, b) \leq L_1 \\ wr_i(t), & \text{if } L_1 \leq rand_i(l, b) \leq L_2 \\ nq_i(t) \text{ or } wr_j(t), & \text{otherwise.} \end{cases} \quad (3)$$

In this scenario, tnq is a prospective source of food for the new queen that is generated from the equation. Obviously, the old queen bee would be the best choice if the question was answered with a q . If the options wr_i and wr_j are chosen, the employees are the most likely candidates to be the feeder. The brooders are a likely option for feeders in the nq scenario.

- Mutation phase: The VNS method is used to execute mating during the mutation phase. After the procedure is completed, the new queens exit the hive.
- Mating phase: Drones per colony are determined using the following equation:

Number of Drones Per Colony =

$$\frac{\text{Number of Drones}}{\text{Number of Queens}} \quad (4)$$

To find a new queen to mate with, the drones must leave the hive and go out into the wild. When the drones depart the home, the ILS algorithm is used.

- Next Iteration: The best-fertilized bees are left behind for the next generation of bees.

In the proposed method, bumble bee optimization algorithm searches the optimal secret data order. The optimal secret data order such as original form, flip, rotate, and complement form are taken under consideration. The

2.2 Least Significant Bit (LSB) Algorithm

In the LSB algorithm, the least significant bit of the cover image pixel is replaced with secret data bit, as shown in Figure 2 [17]. Further, k -bit LSB algorithm is developed from it by replacing the k -LSB bits of the cover image with secret data bit. The k -bit LSB algorithm provides better embedding capacity over LSB algorithm but provides more variability in the cover image.

10100011	10101100	00110011	00001111
(a) Cover Image Pixels			
0	1	1	0
(b) Secret Data Bits			
1010001 <u>0</u>	1010110 <u>1</u>	0011001 <u>1</u>	0000111 <u>0</u>
(c) Stego Image Pixels			

Figure 2 LSB Algorithm

3. PROPOSED METHOD

The proposed method reduces the variability to enhance the imperceptibility in the image steganography. The flowchart of the proposed

method is shown in Figure 1. Initially, secret data and cover images are read. After that, optimal cover image is determined by determining the 0's and 1's probability in the LSB of cover images.

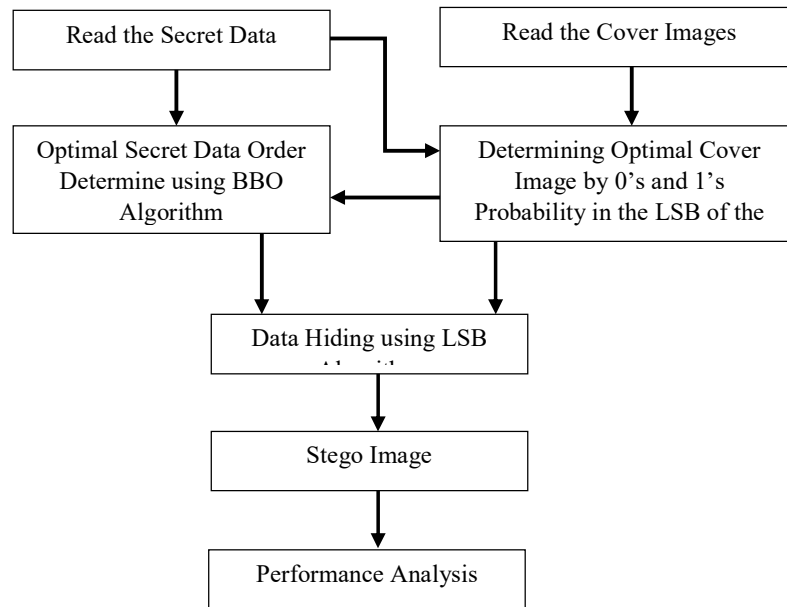


Figure 3 Block Diagram of the Proposed Method

Out of all cover images, which cover image 0's and 1's probability is near about the secret data 0's and 1's probability that cover image is chosen as optimal cover image. Next, bumble bee optimization (BBO) algorithm is deployed for determine optimal secret data order. BBO algorithm based on the objective function determine the optimal secret data order which provides minimum variability in the optimal cover image. Further, determining the optimal secret data order, the data hiding is done in the cover image using the LSB algorithm that gives the stego image in the output. In the last, performance analysis of the proposed method is done using various performance parameters such as mean square error (MSE), peak signal to noise ratio (PSNR), and embedding capacity (EC).

4. SIMULATION EVALUATION

The proposed method is simulated in MATLAB. The system configuration is Intel core, i7 processor, 2.90GHz, 8GB RAM, and 64-bit operating system.

4.1 Simulation Setup Configuration

In this section, simulation setup configurations are explained for the proposed method.

Parameters	Value
Total Population	50
Iterations	50
Lower Bound	1
Upper Bound	4
Fitness Function	PSNR
Cover Image Size	256x256
Secret Data	64x128



Table 1 Simulation Setup Configuration

4.2 Performance Parameter

In this section, we have explained the performance parameters calculated for the proposed method [18].

- Mean Square Error (MSE): This parameter calculates the mean square error between cover and stego image using Eq. (5).

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H (X_{ij} - Y_{ij})^2 \quad (5)$$

Here, W specifies the width of image specified in pixels and similarly, H specifies the height. X_{ij} specify the pixel value of carrier image at point (i,j) and y_{ij} specify the pixel value of stego image at point (i,j). The smaller the MSE score, the less the mean difference between the images. When two images are identical, the MSE is 0.

- Peak Signal to Noise Ratio (PSNR): To put it simply, PSNR measures the difference in intensity values between the stego image and carrier image before and after compression. Stego images with a higher PSNR value show less distortion, which means the images are of greater quality. The PSNR statistic is described as follows:

$$PSNR = 10 \log_{10} \frac{P^2}{MSE} \quad (6)$$

- Embedding Capacity: This parameter measures how many bits can be embedded in the cover image. It is calculated in bits per pixel (bpp).

$$EC = \frac{\text{Total Bits Embedded}}{\text{Total Pixels in the Image}} \quad (7)$$

4.3 Simulation Results

In this section, we have shown the simulation results of the proposed method and comparative analysis with the existing methods.

Table 2 shows the selected cover image and secret data order is chosen using bumble bee optimization algorithm for data hiding. The results show that the female is the most preferred cover image whereas secret data order 2 is most chosen for data hiding. Besides that, difficult for the attacker to recover secret data without knowing original cover image and secret data order.

Table 2 Selected Cover Images and Secret Data Order

Secret Images	Cover Image	Secret Order	Data
Lena	Female	2	
Baboon	Baboon	4	
Barbara	Female	2	
Pepper	Female	2	
Lake	Baboon	5	

Table 3 shows the mean square error for different secret images. The result shows that on average 0.24456 MSE achieved by proposed method.

Table 3 Mean Square Error (MSE)

Secret Images	MSE
Lena	0.2461
Baboon	0.2464
Barbara	0.2439
Pepper	0.2440
Lake	0.2424
Average	0.24456

Table 4 shows the PSNR for different secret images. The result shows that the proposed method achieves on average 54.252dB.

Table 4 Peak Signal to Noise Ratio (PSNR)

Secret Images	PSNR (in dB)
Lena	54.22
Baboon	54.22
Barbara	54.26
Pepper	54.27
Lake	54.29
Average	54.252

Table 5 shows the embedding capacity of the proposed method. The results show that the proposed method achieves 1bpp.

Table 5 Embedding Capacity

Secret Images	Embedding Capacity (in bpp)
Lena	1
Baboon	1
Barbara	1
Pepper	1



Lake	1
------	---

4.3.1 Comparative Analysis

In this section, the proposed method is compared with the existing method based on PSNR parameter in Table 6. The result shows that the proposed method provides better PSNR over the existing method.

Table 6 Comparative Analysis based on PSNR Parameter

Secret Images	Pratik D. Shah and Rajankumar S. Bichkar [15]	Proposed Method
Lake	52.17dB	54.29dB
Pepper	52.25dB	54.27dB

5. CONCLUSION AND FUTURE SCOPE

In this paper, bumble bee optimization (BBO) algorithm is deployed for optimized data hiding in image steganography. To achieve this goal, PSNR is used as an objective function and based on this function, the BBO algorithm searches the optimal secret data order. After determining the optimal secret data order, LSB based data hiding is done. Besides that, optimal cover image is also determined. The proposed method simulation evaluation is done on USC-SIPI digital image database. The results show that the proposed method the cover image and secret data is order for different. Thus, difficult for the attacker to recover secret data from the cover image. On the other side, the proposed method provides better imperceptibility in terms of PSNR as compared to the existing method. In the future, we will work on other parameters of steganography such as data hiding capacity and robustness against attacks. To achieve this goal, we will explore data compression and error correction code (ECC) algorithms.

REFERENCES

[1] Muhammad, K., Ahmad, J., Rehman, N.U., Jan, Z. and Sajjad, M., 2017. CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, 76(6), pp.8597-8626.

[2] Subramanian, N., Elharrouss, O., Al-Maadeed, S. and Bouridane, A., 2021. Image steganography: A review of the recent advances. *IEEE Access*.

[3] Lakshmi Sirisha, B. and Chandra Mohan, B., 2021. Review on spatial domain image steganography techniques. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(6), pp.1873-1883.

[4] ALabaichi, A., Al-Dabbas, M.A.A.A.K. and Salih, A., 2020. Image steganography using least significant bit and secret map techniques. *International journal of electrical & computer engineering (2088-8708)*, 10(1).

[5] Huang, H.C., Chang, F.C., Chen, Y.H. and Chu, S.C., 2015. Survey of Bio-inspired Computing for Information Hiding. *J. Inf. Hiding Multim. Signal Process.*, 6(3), pp.430-443.

[6] Kanan, H.R. and Nazeri, B., 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. *Expert systems with applications*, 41(14), pp.6123-6130.

[7] De Carvalho, R.L., Da Silva, W.G. and De Moraes, A.H.O., 2017. Optimizing image steganography using particle swarm optimization algorithm. *International Journal of Computer Applications*, 164(7).

[8] Nassr, D.I. and Khamis, S.M., 2021. Applying Permutations and Cuckoo Search for Obtaining a New Steganography Approach in Spatial Domain. *International Journal of Network Security*, 23(1), pp.67-76.

[9] Wang, Z.H., Chang, C.C. and Li, M.C., 2012. Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences*, 192, pp.98-108.

[10] Karmakar, A. and Agarwal, A., 2021. Optimized Data Hiding Technique Using Egyptian Vulture Optimization Algorithm For Image Steganography. *Design Engineering*, pp.12525-12541.

[11] Shah, P.D. and Bichkar, R.S., 2018. A secure spatial domain image steganography using genetic algorithm and linear congruential generator. In *International conference on intelligent computing and applications* (pp. 119-129). Springer, Singapore.

[12] Khamrui, A., Gupta, D.D., Ghosh, S. and Nandy, S., 2017, March. A Spatial Domain Image Authentication Technique Using Genetic Algorithm. In *International Conference on Computational Intelligence, Communications, and*





Business Analytics (pp. 577-584). Springer, Singapore.

[13] Soleimanpour-Moghadam, M. and Talebi, S.I.A.M., 2013. A novel technique for steganography method based on improved genetic algorithm optimization in spatial domain. *Iranian Journal of Electrical and Electronic Engineering*, 9(2), pp.67-75.

[14] Shah, P.D. and Bichkar, R.S., 2021. Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. *Engineering Science and Technology, an International Journal*, 24(3), pp.782-794.

[15] Shah, P.D. and Bichkar, R.S., 2020, June. Genetic Algorithm based Approach to Select

Suitable Cover Image for Image Steganography. In *2020 International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.

[16] Marinakis, Y., Marinaki, M. and Migdalas, A., 2017. An adaptive bumble bees mating optimization algorithm. *Applied Soft Computing*, 55, pp.13-30.

[17] Banharnsakun, A., 2018. Artificial bee colony approach for enhancing LSB based image steganography. *Multimedia Tools and Applications*, 77(20), pp.27491-27504.

[18] Wazirali, R., Alasmay, W., Mahmoud, M.M. and Alhindi, A., 2019. An optimized steganography hiding capacity and imperceptibly using genetic algorithms. *IEEE Access*, 7, pp.133496-133508.